"Elastic Security"

Jean-Marc Pouchoulon

septembre 2025

Elastic security est une suite de sécurité qui permet de collecter des logs, de les analyser et de les visualiser. La suite est libre sauf pour certaines fonctionnalités avancées comme le "machine learning" et intègre des dashboards sécurité. Les "logs" sont collectés dans le but de permettre la détection d'intrusion à l'aide de règles fournies par Elastic ou par la communauté et de vos propres règles.

1 Mise en place d'un environnement Elastic Security

Docker doit être installé sur votre machine. L'environnement Elastic est composée de plusieurs conteneurs docker.

Faire un "git clone `https://github.com/pushou/siem.git`" afin d'installer "elastic SIEM" , l'IDS "Suricata", Evebox, et Zeek. La configuration nécessaire est musclée et une machine avec 16Go de Ram est un minimum.*

Vous obtiendrez de l'aide en lançant la commande "make help".

Modifiez le fichier /etc/sysctl.conf

```
vm.max_map_count=262144
```

Puis faire

```
systctl -p
```

ElasticSearch demande 10% d'espace disque libre pour fonctionner. La procédure d'installation désactive ce contrôle mais ne l'oubliez pas si vous installez ElasticSearch sur une machine de production.

Vous lancerez les commandes suivantes pour installer les différents composants.

```
make es
# ...attendez que la procédure soit terminée, les autres "containers" en ont besoin pour démarrer
make siem
make fleet
```

"make pass" vous permettra de visualiser le mot de passe pour l'utilisateur "elastic" qui est le super utilisateur de la suite.

"make clean" vous permettra de supprimer tous les conteneurs docker.

Vous pouvez vous connecter à l'interface web de la suite à l'adresse `https://ip_de_votre_machine:5601` avec le compte "elastic" et le mot de passe obtenu précédemment. La stack elastic que vous venez d'installer est composée des éléments suivants :

- Une instance d'Elasticsearch: moteur de recherche et de stockage des données qui écoute sur le port 9200 en TLS sur votre hôte.
- Une instance Kibana: interface web pour visualiser les données qui écoute sur le port 5601 en TLS sur votre hôte.
- Une instance fleet: interface web pour gérer les agents Elastic ou Beats qui écoute sur le port 8220 en TLS sur votre hôte.

L'IPS "Suricata" est aussi installé sous forme de container et va suivre les flux réseaux de votre machine hôte. Les alertes "Suricata" sont envoyées à Elasticsearch et sont visualisables via Kibana.

2 Configuration de fleet

2.1 Configuration de l'url de fleet

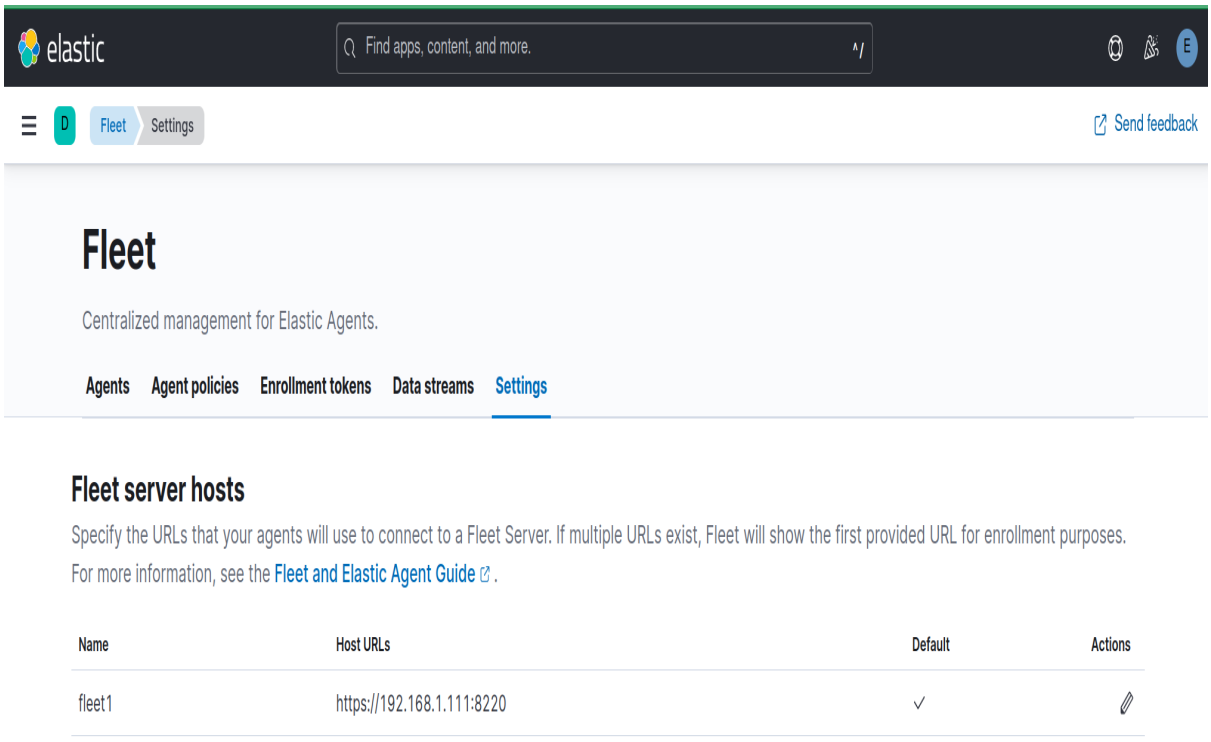

FIGURE 1 – Configuration de l'url de fleet.

2.2 Configuration des "outputs" de fleet

Utilisez "make fgprint" et "make prca" dans la directory clonée au départ du TP afin de récupérer le fingerprint et le certificat de votre AC fleet.

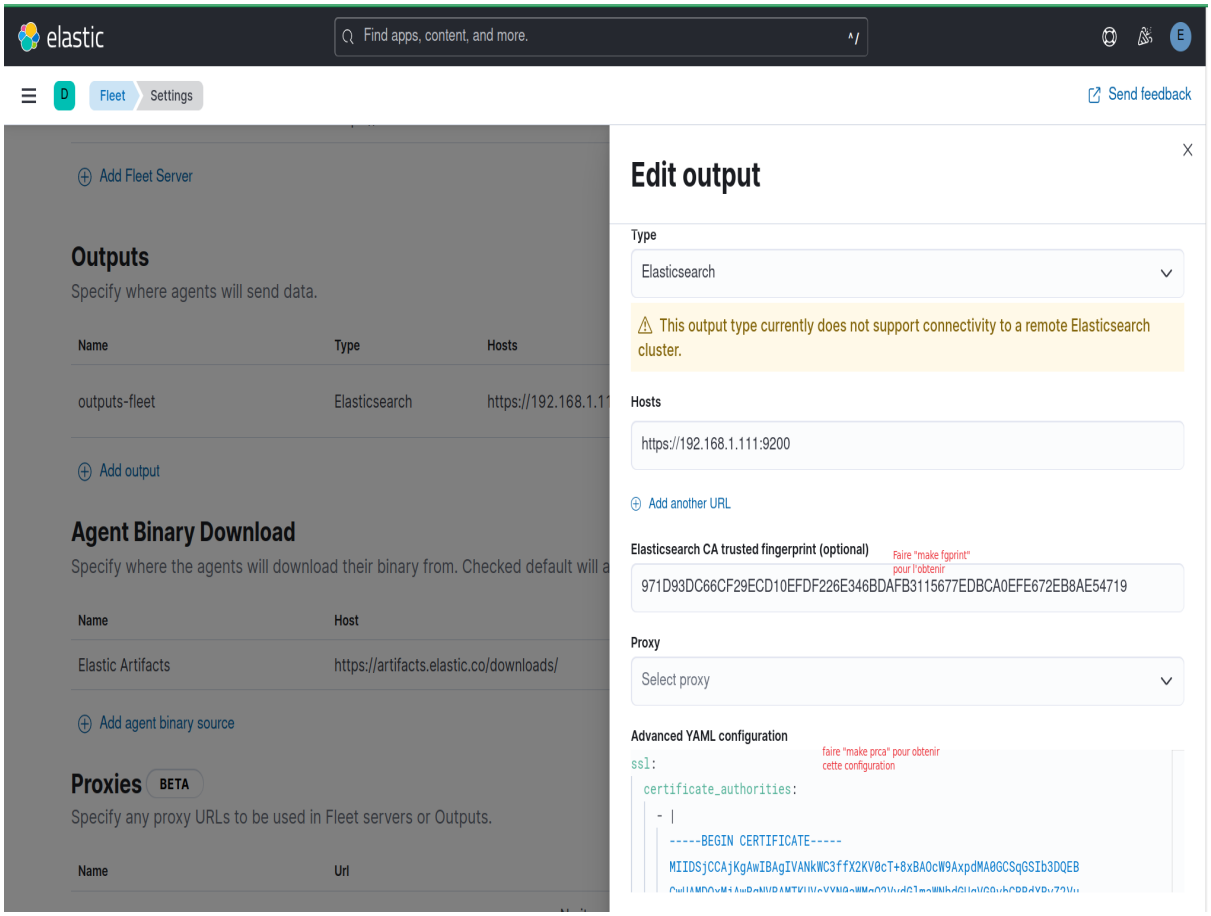

FIGURE 2 – Configuration des "outputs" de fleet.

3 Agent Elastic sur un poste Windows

3.1 Installation de l'agent Elastic sur un poste Windows

N'oubliez pas de désactiver le pare-feu de votre poste Windows et l'antivirus "Microsoft Defender".

Installer l'"elastic agent" sur un poste windows (VM ou physique du CloudLab) et connectez-le à votre "fleet server". Pour cela, suivez le menu "add agent" de fleet qui vous donnera la commande "Powershell" pour le faire. Vous créerez une "policy Windows" standard et vous l'appliquerez à votre agent.

L'adresse de connexion à Elastic est `https://ip_de_votre_machine:9200`: n'utilisez pas localhost ! Lors de l'installation de l'agent, rajoutez l'option –insecure pour désactiver la vérification du certificat du serveur Elastic.

3.2 Déploiement des intégrations pour Windows

Charger les deux intégrations suivantes:

- titre "Windows"
- titre "Elastic Defend"

Vous appliquerez ces deux intégrations à l'agent déployé.

3.3 Configuration de l'"intégration" de "Defend"

Dans un premier temps passer l'integration "Defend" en mode "detect". Faite ensuite de même pour la vérification du hostname.

3.4 Retrouvez des informations sur votre poste Windows

1. Retrouvez les métriques systèmes de votre poste Windows dans Kibana (voir menu "hosts").
2. Retrouvez les métriques sur les services de votre machine Windows.
3. Retrouvez les pourcentages des différents type d'évènements windows ("security" , "sysmon" ...) de votre machine dans Kibana
4. Retrouvez les alertes liées à Suricata.

Vous pouvez tester la connectivité de votre agent fleet via la commande:

```
.\elastic-endpoint.exe test output
```

Vous pouvez afficher les logs de l'agent avec la commande:

```
.\elastic-endpoint.exe logs -f
```

Vous pouvez afficher la configuration de l'agent avec la commande:

```
.\elastic-endpoint.exe inspect
```

3.5 Lancez et détectez une simulation d'attaques

1. Chargez et faites "enable" de toutes les règles de détection fournies en standard par Elastic. Seules celles nécessitant un abonnement ne seront pas activées.
2. Clonez le "repository" suivant dans votre machine windows : `https://github.com/NextronSystems/APTSimulator`.
3. Lancez le script "APTSimulator.bat" en mode administrateur et lancez toutes les simulations d'attaques pour faire réagir l'agent.
4. Vérifiez que vous avez bien des alertes dans la partie "Security" de Kibana.
5. Créez une timeline sur l'alerte "process creation". Analyser cet évènement avec Kibana pour obtenir un joli graphique.
6. Remettez "Defend" en mode "prevent" et relancez les simulations d'attaques. Vérifiez que les attaques sont bloquées.

4 Agent Elastic sur un poste Linux

Si vous ne voulez pas utiliser l'option "insecure" pour l'agent Elastic, vous devrez installer un certificat de votre autorité de certification sur votre poste Linux.

```
sudo cp ./temp/ca.crt /usr/local/share/ca-certificates/ca.crt
sudo update-ca-certificates
```

1. Installez l'agent Elastic sur un poste Linux (VM ou physique du CloudLab) et connectez-le à votre "fleet server" comme vous l'avez fait pour l'agent Windows.
2. Installez et visualiser les tableaux de bord produits par l'intégration "audit manager". (auditd ne doit pas être activé sur votre poste Linux).

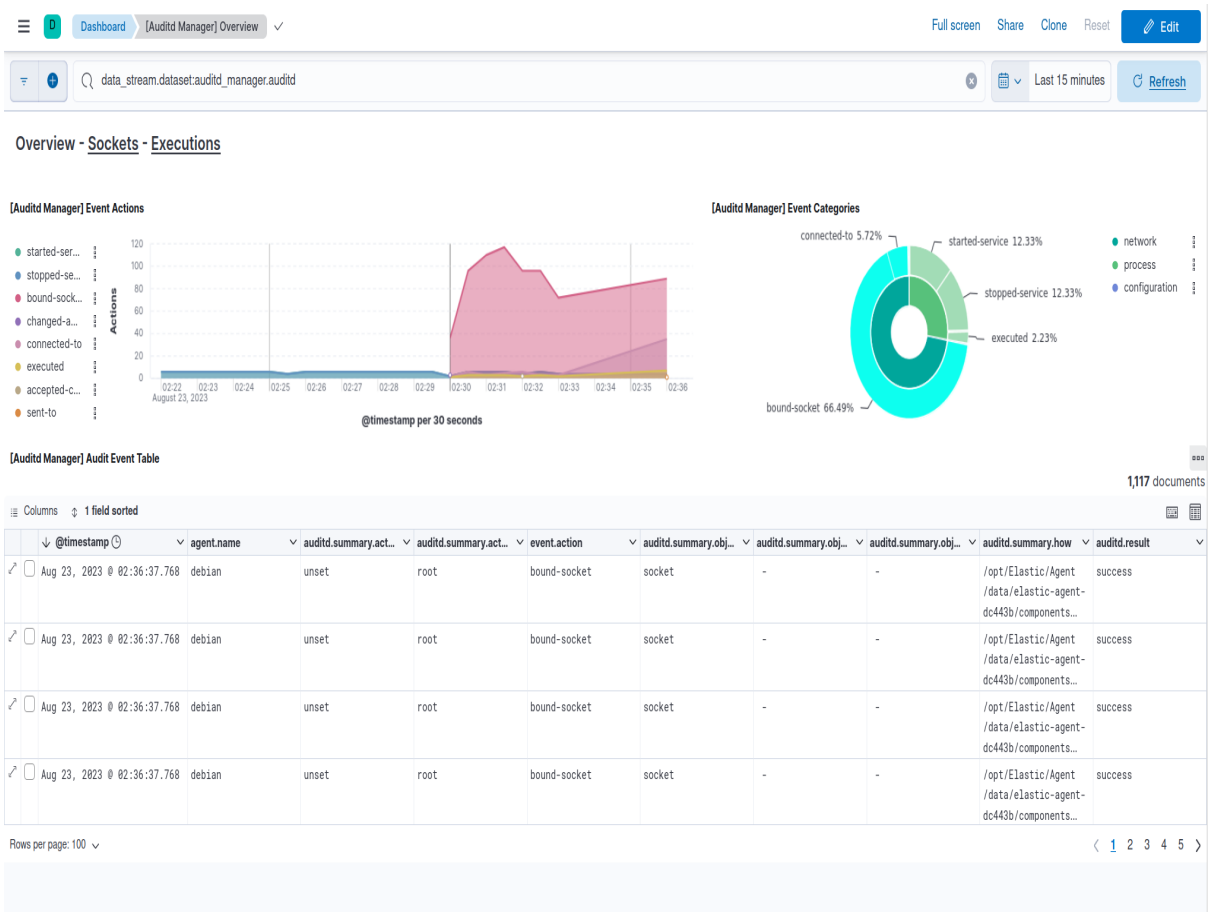

FIGURE 3 – Résultat de l'"intégration" d'auditd.

3. Installez "Sysmon for Linux". voir `https://github.com/Sysinternals/SysmonForLinux/blob/main/INSTALL.md`
4. Installez et visualiser le tableau de bord de l'intégration "Sysmon for Linux". Ajouter /var/log/-syslog dans les logs à collecter dans l'intégration

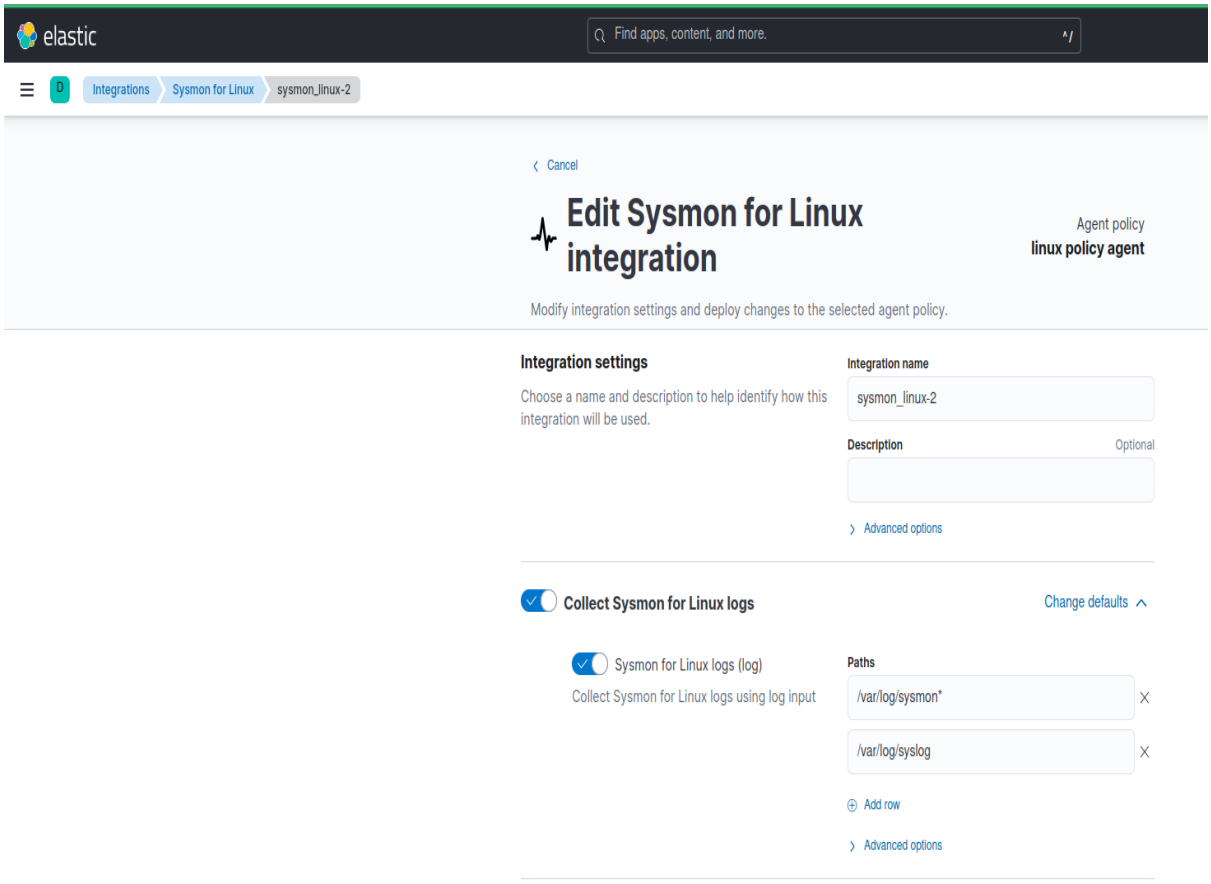

FIGURE 4 – Configuration de l'intégration de "Sysmon for Linux".

Visualiser le résultat:

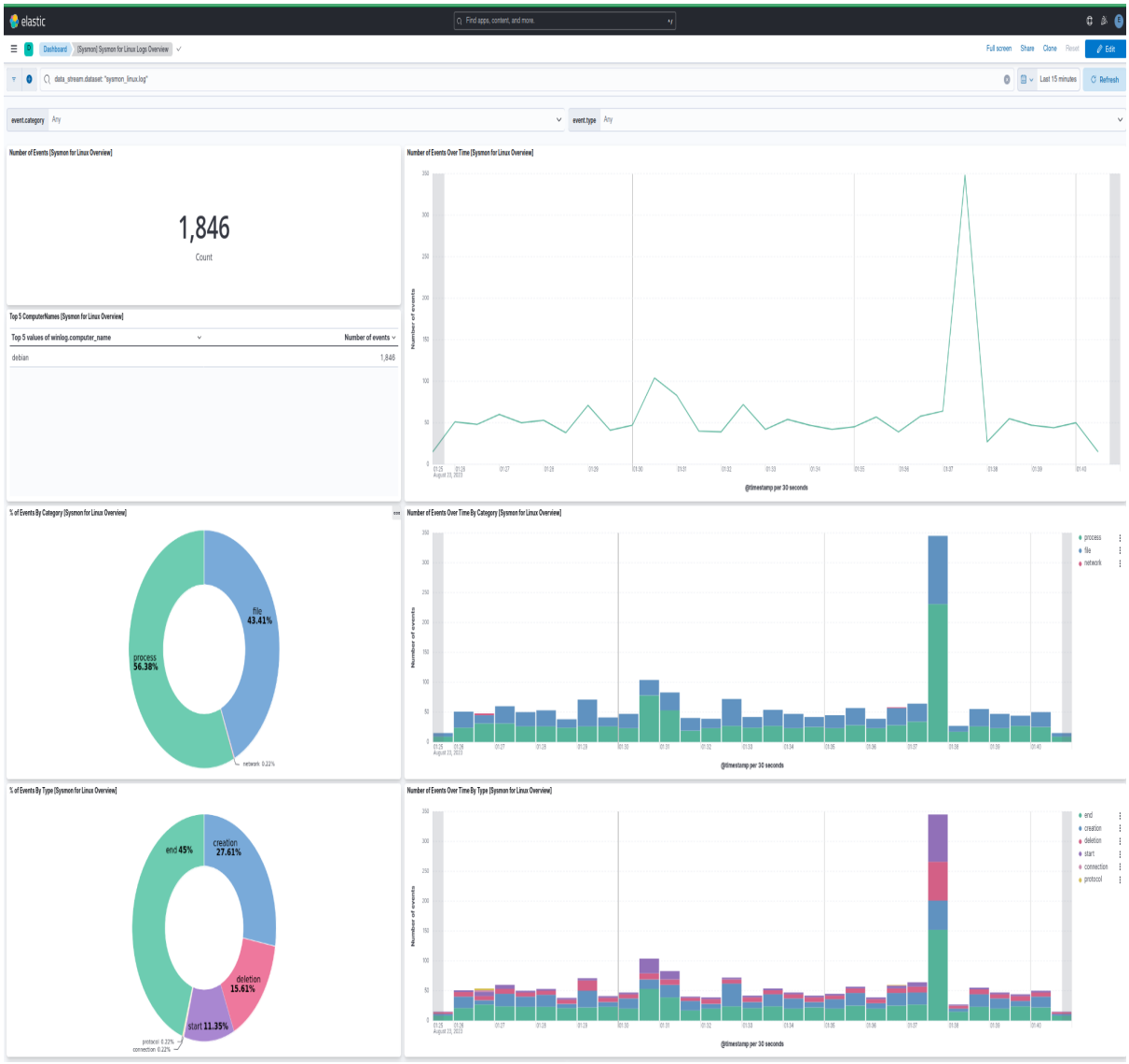

FIGURE 5 – Tableau de bord de l'intégration de "Sysmon for Linux".

5 Installation de l'Application Performance Monitoring (APM) d'Elastic sous Linux

On se propose ici d'installer l'Application Performance Monitoring (APM) de Elastic sur un poste Linux. Il s'agit des mêmes technologies que pour les agents Elastic mais avec des fonctionnalités orientées "performance applicatives".

Une norme concernant l'observabilité des applications est en train de se mettre en place: OpenTelemetry. Ce framework permet de collecter des métriques, des traces et des logs de vos applications quelque soit l'outil de monitoring utilisé. Ici on utilisera l'agent Elastic pour collecter les métriques de notre application et l'intégration APM de Elastic pour les visualiser.

5.1 pré-requis et installation

Vous devez avoir installé une VM avec au moins 50 Go de disque et 24 gigas de RAM.

1. Installez comme précédemment la suite Elastic avec un serveur fleet et une agent Elastic sur votre VM Linux.
2. Clonez l'application de démonstration de `https://github.com/elastic/opentelemetry-demo.git`
3. Modifiez le fichier src/otelcollector/otelcol-elastic-config-extras.yaml pour ajouter le nom de votre serveur Elastic:

```
otlp/elastic:
endpoint: "http://ADRESSE\_DE\_VOTRE\_VM:8200"
compression: none
tls:
  insecure: true
```

4. Lancez l'application de démonstration avec la commande "make start"
5. Déployez l'intégration "APM" sur votre serveur Elastic. intégration "APM":

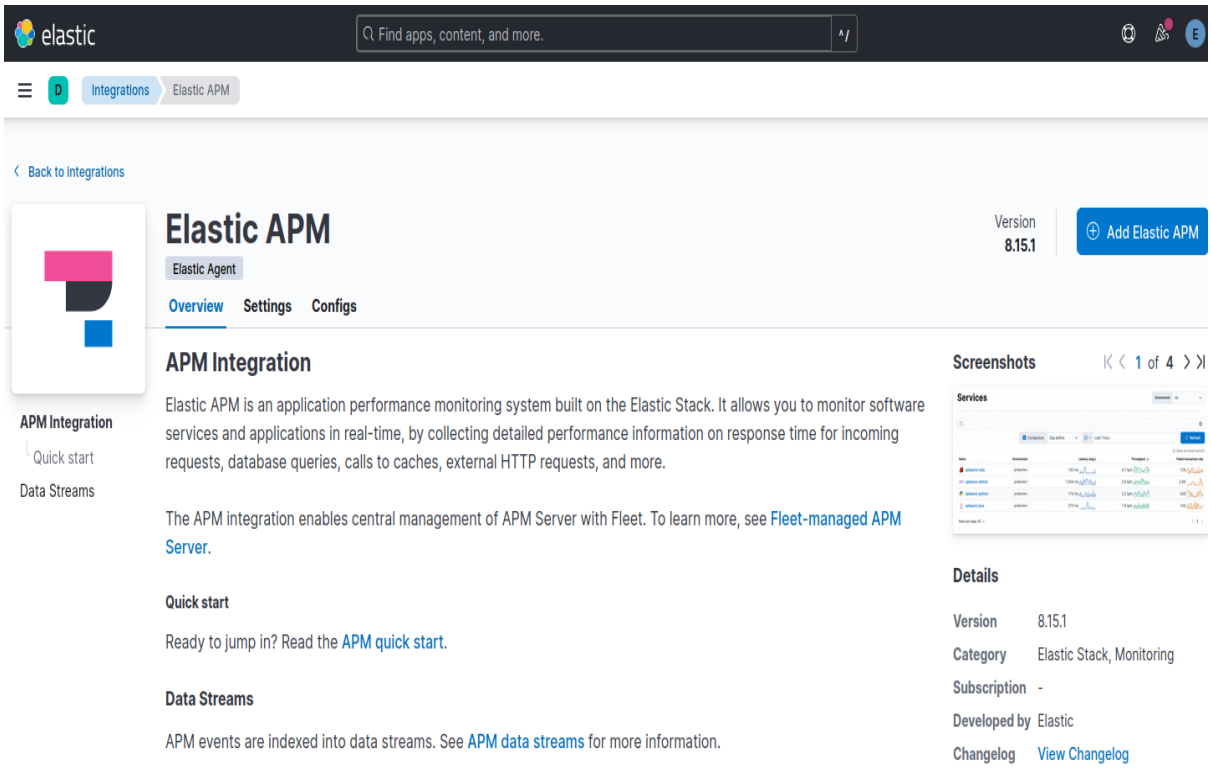

FIGURE 6 – Configuration des "outputs" de fleet.

Configuration de l'intégration "APM":

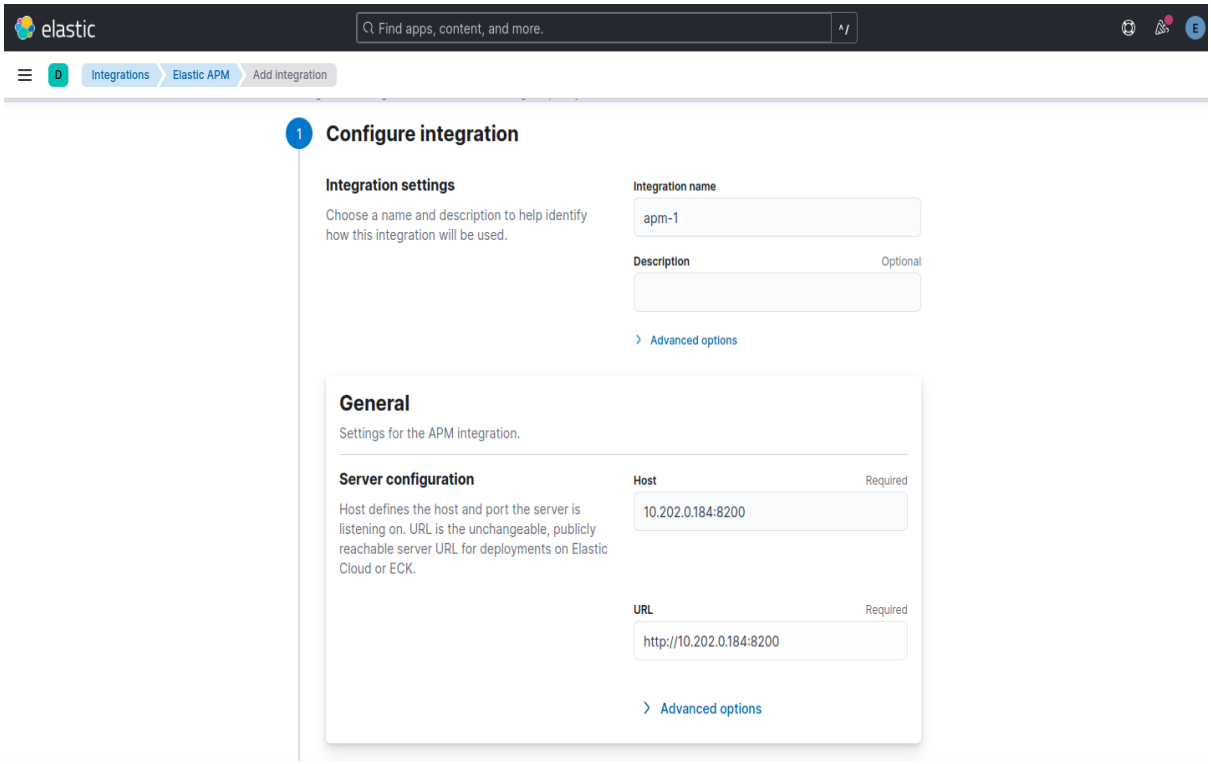

FIGURE 7 – Configuration des "outputs" de fleet.

Configuration de l'intégration "APM":

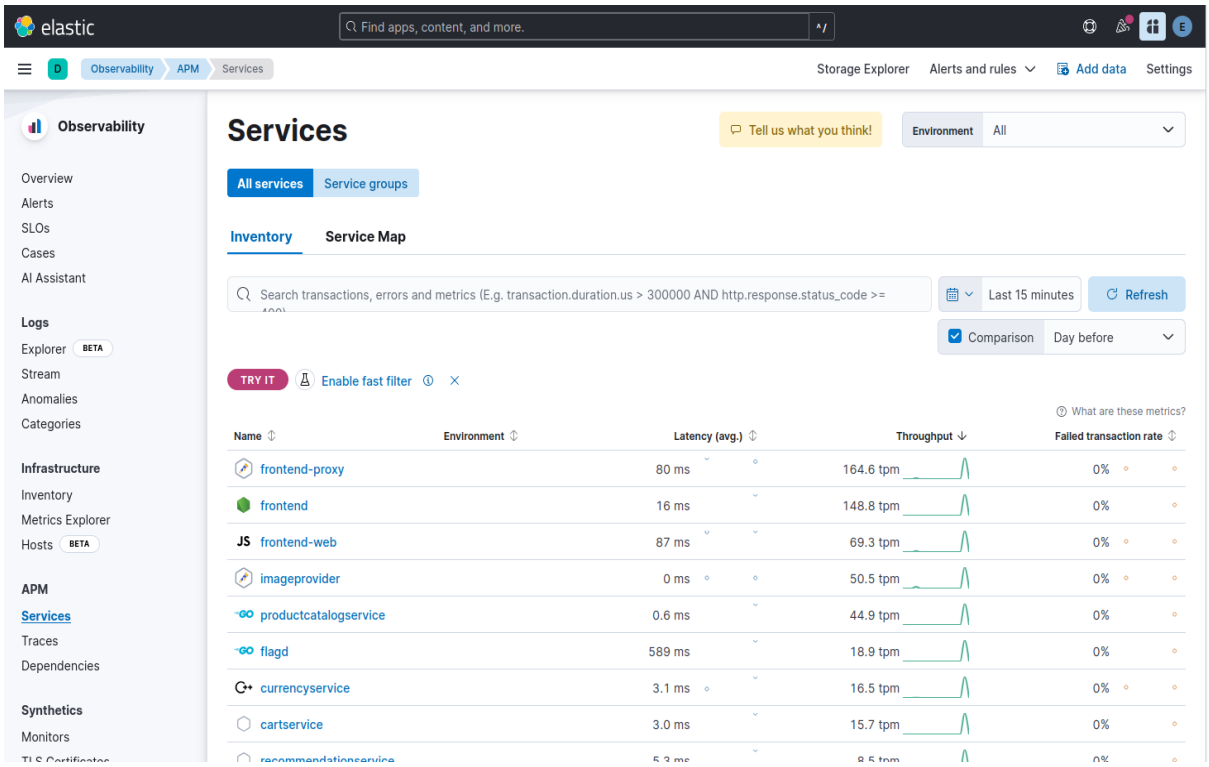

FIGURE 8 – Configuration des "outputs" de fleet.

Visualisez les métriques de votre application: Configuration de l'intégration "APM":

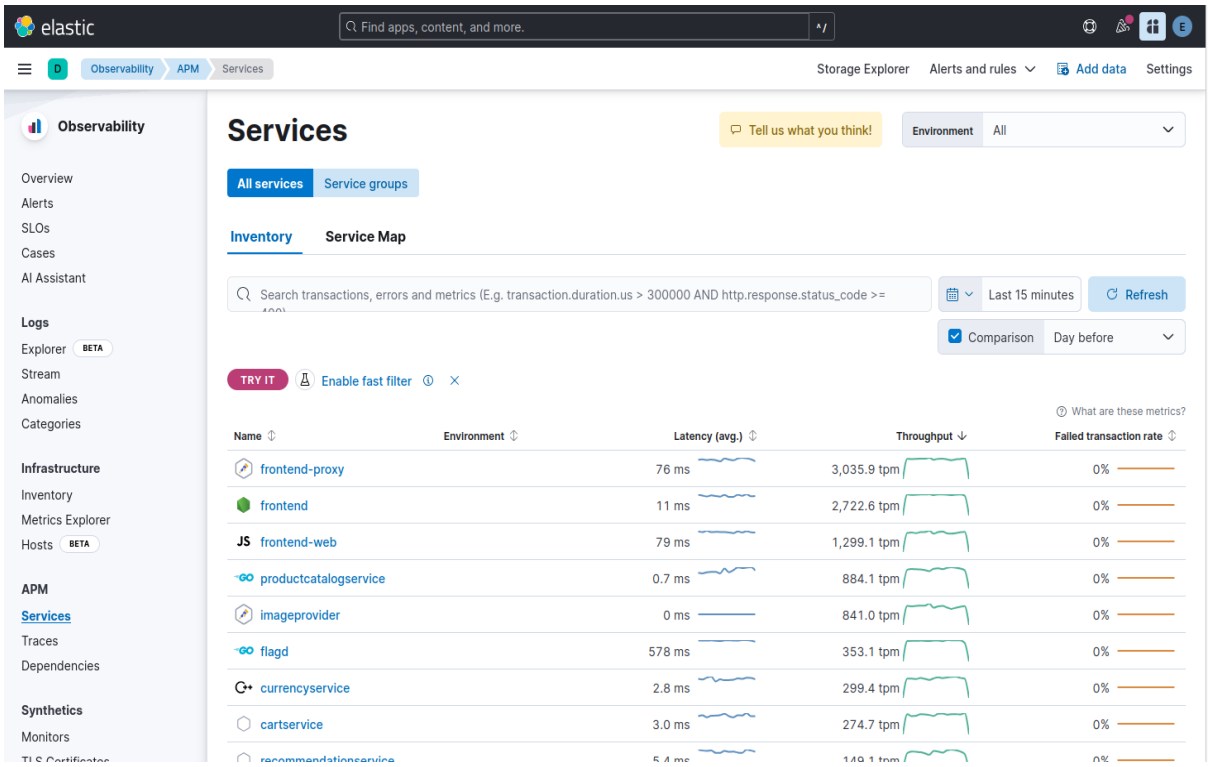

FIGURE 9 – Configuration des "outputs" de fleet.